handleiding Desktop Management

hp workstation xw4000
hp workstation xw6000

Artikelnummer van het document: 301201-331

Oktober 2002

Deze handleiding bevat definities en instructies voor het gebruik van de beveiligingsvoorzieningen en van Intelligent Manageability (Compaq Client Management) die vooraf zijn geïnstalleerd op bepaalde modellen.

WAARSCHUWING: Als u de aanwijzingen na dit kopje niet opvolgt, kan dit leiden tot persoonlijk letsel of levensgevaar.

VOORZICHTIG: Als u de aanwijzingen na dit kopje niet opvolgt, kan dit leiden tot beschadiging van de apparatuur of verlies van gegevens.

---

handleiding Desktop Management
hp workstation xw4000
hp workstation xw6000
Eerste editie (oktober 2002)
Artikelnummer van het document: 301201-331

Inhoudsopgave

Handleiding Desktop Management

Index

Handleiding Desktop Management

HP heeft in 1995, met de introductie van de eerste desktopcomputers die volledig konden worden beheerd, het voortouw genomen op het gebied van desktop management. Sindsdien heeft HP het voortouw genomen in de ontwikkeling van de standaarden en infrastructuur die nodig zijn om desktopcomputers, werkstations en notebookcomputers efficiënt te kunnen toepassen, configureren en beheren. HP Intelligent Manageability (HP Client Management) biedt op standaarden gebaseerde oplossingen voor het beheren en besturen van desktopcomputers, werkstations en notebookcomputers in een netwerkomgeving. HP werkt nauw samen met vooraanstaande fabrikanten van beheersoftware ter bevordering van de compatibiliteit tussen Intelligent Manageability en deze producten. Intelligent Manageability maakt een belangrijk onderdeel uit van onze inspanningen op velerlei gebied om u te voorzien van oplossingen voor de vier fasen van de levenscyclus van een desktopcomputer: planning, implementatie, beheer en overgang.

In deze handleiding worden de mogelijkheden en functies van de zeven belangrijkste onderdelen van desktop management samengevat:

- Eerste configuratie en gebruik
- Systeeminstallatie op afstand
- Updates en beheer van software
- ROM-flash
- Bouwstenen en partners
- Inventarisbeheer en beveiliging
- Foutmeldingen en foutherstel

De ondersteuning voor specifieke functies die in deze handleiding worden beschreven, varieert per model of softwareversie.

Eerste configuratie en gebruik

Uw computer wordt geleverd met een vooraf geïnstalleerd image van de systeemsoftware. Na een korte procedure waarin de software wordt "uitgepakt", is de computer gereed voor gebruik.

Desgewenst kunt u de vooraf geïnstalleerde software vervangen door aangepaste systeem- en applicatiesoftware. Aangepaste software kan op verschillende manieren worden geïmplementeerd. Enkele manieren zijn:

- Extra applicaties installeren nadat u het vooraf geïnstalleerde software-image heeft uitgepakt;
- De vooraf geïnstalleerde software vervangen door een aangepast software-image met speciale hulpprogramma's voor software-installatie, zoals Altiris eXpress, Microsoft MS Batch of Microsoft NT Distribution Share (NTDS);
- De inhoud van een vaste schijf naar een andere vaste schijf kopiëren via een kloonproces.

Wat de beste methode voor implementatie is, hangt af van uw IT-omgeving en IT-processen. Het gedeelte PC Deployment op de website Solutions and Services (http://www.compaq.com/solutions/pcsolutions) bevat informatie aan de hand waarvan u de beste installatiemethode kunt selecteren. Hier vindt u ook handleidingen en hulpprogramma's voor de integratie van installatieprogramma's van Microsoft of op PXE gebaseerde installatieprogramma's.

De cd *Compaq Restore* (of *Restore Plus!*), het ROM-configuratieprogramma en ACPI-hardware helpen u verder bij het herstellen van de systeemsoftware, het configuratiebeheer, het oplossen van problemen en energiebeheer.

Remote System Installation

Met Remote System Installation (Systeeminstallatie op afstand) kunt u het systeem opstarten en instellen met behulp van de software en configuratiegegevens die op een netwerkserver aanwezig zijn. Deze voorziening wordt gewoonlijk gebruikt als hulpmiddel voor het instellen en configureren van een systeem en kan voor de volgende taken worden gebruikt:

- Software-image installeren op een of meer nieuwe computers.
- Vaste schijf formatteren.
- Applicaties of stuurprogramma's installeren.
- Het besturingssysteem, de applicatiesoftware of de stuurprogramma's bijwerken.

U start Remote System Installation door op **F12** te drukken zodra het bericht F12 = Network Service Boot (Netwerk-opstartbeveiliging) rechtsonder in het scherm met het HP logo verschijnt. Volg de instructies op het scherm om door te gaan.

HP en Altiris, Inc. hebben de krachten gebundeld om hulpprogramma's te maken die bedoeld zijn om de implementatie en het beheer van bedrijfscomputers gemakkelijker en minder tijdrovend te maken. Hierdoor worden uiteindelijk de exploitatiekosten lager en zijn HP computers de best te beheren clientcomputers in de bedrijfsomgeving.

Software bijwerken en beheer

HP biedt verschillende hulpmiddelen voor het beheren en bijwerken van software op desktopcomputers en workstations: Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris HP/Compaq Client Manager, System Software Manager, Product Change Notification en ActiveUpdate.

Altiris eXpress

HP en Altiris hebben hun samenwerking geïntensiveerd teneinde geavanceerde oplossingen te kunnen leveren voor een eenvoudiger beheer van hardware en software voor desktopcomputers, notebookcomputers, handheld apparaten en servers gedurende de gehele levenscyclus. Met Altiris eXpress kan de systeembeheerder gemakkelijk en snel een aan de bedrijfsstandaard aangepast software-image installeren op een of meer netwerkclients, via een interface die net zo eenvoudig werkt als Windows Verkenner. Altiris eXpress ondersteunt Wired for Management en Preboot Execution Environment (PXE) van Intel. Met Altiris eXpress en de Remote System Installation voorzieningen van de HP computer kan de systeembeheerder op elke nieuwe computer het software-image installeren zonder naar deze computer toe te hoeven gaan.

De oplossingen van Altiris eXpress bieden een efficiënte en effectieve manier om bestaande processen te automatiseren en knelpunten binnen uw IT-omgeving op te lossen. Met de webgeoriënteerde infrastructuur van Altiris eXpress beschikt u over de flexibele mogelijkheid om uw systemen op elk gewenst moment vanaf elke locatie te beheren – zelfs vanaf een iPAQ Pocket PC!

De oplossingen van Altiris eXpress zijn modulair opgebouwd en uitbreidbaar, zodat ze kunnen voorzien in de behoeften op werkgroepniveau én op het niveau van de onderneming. Deze oplossingen kunnen worden geïntegreerd met andere standaardpakketten voor clientmanagement en ze vormen een uitbreiding op Microsoft BackOffice/SMS.

De uitgebreide oplossingen van Altiris eXpress zijn geconcentreerd rond vier centrale IT-thema's:

- Implementatie en migratie
- Software- en operationeel beheer
- Inventarisbeheer
- Helpdesk en probleemoplossing

De installatie van Altiris eXpress duurt slechts enkele minuten. Daarna kunt u een schijf-image installeren dat het besturingssysteem, applicatiesoftware en de Altiris eXpress-client bevat, zonder dat u een aparte opstartdiskette nodig heeft. Met Altiris eXpress kan de netwerkbeheerder het volgende doen:

- Een nieuw image maken of een bestaand image bewerken of een netwerkcomputer met het ideale image klonen.
- Een onbeperkt aantal aangepaste schijf-images maken voor verschillende werkgroepen.
- Image-bestanden bewerken en ze wijzigen zonder helemaal opnieuw te hoeven beginnen. Dit is mogelijk doordat de bestanden door Altiris eXpress in de oorspronkelijke indeling worden opgeslagen: NTFS, FAT16 of FAT32.
- Een script voor nieuwe computers maken, dat automatisch wordt uitgevoerd wanneer een nieuwe computer in het netwerk wordt opgenomen. Met dit script kunt u bijvoorbeeld de vaste schijf formatteren, een flash uitvoeren van het ROM-BIOS en een compleet, standaard software-image installeren;
- Een gebeurtenis plannen die op verschillende computers moet worden uitgevoerd.

Altiris eXpress bevat ook makkelijke functies voor softwaredistributie. U kunt Altiris eXpress gebruiken voor het bijwerken van besturingssystemen en applicaties vanaf een centrale console. Wanneer u Altiris eXpress gebruikt in combinatie met System Software Manager, kunt u hiermee ook het ROM-BIOS en stuurprogramma's bijwerken.

Voor meer informatie bezoekt u http://www.compaq.com/easydeploy.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro maakt probleemloze computermigratie mogelijk door oude instellingen, voorkeuren en gegevens te bewaren en snel en eenvoudig te migreren naar de nieuwe omgeving. Een upgrade kost nog maar enkele minuten in plaats van uren of dagen, en het bureaublad en de applicaties hebben precies het uiterlijk en de functionaliteit die de gebruikers verwachten.

Bezoek de website http://www.compaq.com/easydeploy voor meer informatie over het downloaden van een gedurende 30 dagen volledig functionele evaluatieversie.

Altiris eXpress HP/Compaq Client Manager

Altiris eXpress HP/Compaq Client Manager biedt een nauwe integratie van HP Intelligent Manageability (Client Management) met Altiris eXpress, hetgeen leidt tot een uitstekende beheerfunctionaliteit voor HP apparaten. Enkele van de beschikbare functies zijn:

- Gedetailleerde overzichten van de hardware-inventaris ten behoeve van het inventarisbeheer.
- Controle en diagnostiek van de toestand van de computer.
- Proactieve informatie over wijzigingen in de hardwareomgeving.
- Meldingen via een webinterface over essentiële gebeurtenissen die zich in de computers hebben voorgedaan, zoals temperatuur-waarschuwingen, geheugenfouten en dergelijke.
- Updates op afstand van systeemsoftware, zoals stuurprogramma's en ROM BIOS.

Voor meer informatie over Altiris eXpress HP/Compaq Client Manager bezoekt u http://www.compaq.com/easydeploy.

System Software Manager

System Software Manager (SSM) is een hulpprogramma waarmee u op meerdere computers tegelijk een update van de systeemsoftware kunt uitvoeren. Wanneer u SSM uitvoert op een clientcomputer, worden de versies van zowel de hardware als de software gedetecteerd, waarna de update van de software wordt uitgevoerd vanaf een centrale opslagplaats. Stuurprogramma's met SSM-ondersteuning worden op de stuurprogramma-website en op de cd met ondersteunende software aangegeven met een speciaal pictogram. Als u het hulpprogramma wilt downloaden of als u meer informatie wilt opvragen over SSM, bezoekt u http://www.compaq.com/im/ssmwp.html.

Product Change Notification

PCN (Product Change Notification) is een HP programma waarmee u op een beveiligde website profielen kunt definiëren om automatisch en proactief bepaalde e-mailberichten te ontvangen:

- E-mailberichten over wijzigingen in hardware en software voor de meeste computers voor zakelijk gebruik en servers.
- E-mailberichten met adviezen aan klanten voor de meeste computers voor zakelijk gebruik en servers.

De PCN website biedt ook de mogelijkheid om in alle productwijzigingsberichten en klantadviezen te zoeken naar informatie over de meeste computers voor zakelijk gebruik en servers.

Als u meer informatie wilt over PCN of uw eigen profiel wilt maken, bezoekt u http://www.compaq.com/pcn.

ActiveUpdate

ActiveUpdate is een clientapplicatie van HP. De ActiveUpdate-client wordt op het lokale systeem uitgevoerd en maakt gebruik van uw gebruikersprofiel om proactief en automatisch software-updates voor de meeste Compaq/HP computers voor zakelijk gebruik en servers te downloaden.

Om meer informatie over ActiveUpdate te krijgen, om de applicatie te downloaden of om uw eigen profiel te maken, bezoekt u http://www.compaq.com/activeupdate.

ROM-flash

De computer heeft een herprogrammeerbaar flash-ROM (Read Only Memory). Door een instelwachtwoord te definiëren in Computer Setup (Computerinstellingen) kunt u voorkomen dat het ROM onbedoeld wordt gewijzigd of overschreven. Dit is belangrijk om de bedrijfszekerheid van de computer te waarborgen. Als u het ROM wilt upgraden, kunt u het volgende doen:

- Bestel een *ROMPaq*™ upgradediskette bij HP.
- Download de meest recente ROMPaq images van de website http://www.compaq.com.

VOORZICHTIG: Zorg ervoor dat u een instelwachtwoord definieert om het ROM maximaal te beschermen. Het instelwachtwoord voorkomt ROM-upgrades door onbevoegden. Met behulp van System Software Manager kan de systeembeheerder het instelwachtwoord voor een of meer computers tegelijk definiëren. Voor meer informatie bezoekt u http://www.compaq.com/im/ssmwp.html.

Remote ROM Flash

Met een ROM-flash op afstand kan de systeembeheerder het ROM van HP computers op afstand veilig upgraden vanaf de centrale beheerdersconsole. Doordat de systeembeheerder deze taak op afstand uitvoert voor meerdere computers tegelijk, is een consistent gebruik van en betere controle op ROM-versies van HP computers in het gehele netwerk mogelijk. Bovendien leidt dit tot een hogere productiviteit en lagere onderhoudskosten.

De computer moet zijn ingeschakeld of op afstand worden geactiveerd om van ROM-flash op afstand te kunnen profiteren.

Voor meer informatie over ROM-flash op afstand raadpleegt u Altiris eXpress HP/Compaq Client Manager of System Software Manager op de website http://www.compaq.com/easydeploy.

FailSafe Boot Block ROM

Het FailSafe Boot Block ROM (FailSafe ROM met opstartblok) zorgt dat het systeem zich kan herstellen in het onwaarschijnlijke geval dat zich een storing voordoet bij het flashen van het ROM, bijvoorbeeld wanneer de stroom uitvalt tijdens een ROM-upgrade. Het opstartblok is een tegen flashen beveiligd gedeelte van het ROM dat bij het inschakelen van het systeem controleert of de systeem-ROM-flash geldig is.

- Als het systeem-ROM geldig is, start het systeem normaal.
- Als het systeem-ROM niet door de controle komt, biedt het FailSafe ROM met opstartblok voldoende ondersteuning om het systeem op te starten vanaf een ROMPaq diskette, waarmee de systeem-ROM van een geldige ROM-versie kan worden voorzien.

Als het opstartblok een ongeldig systeem-ROM ontdekt, geeft het systeem een aantal geluidssignalen (eenmaal lang, driemaal kort) en gaan de drie lampjes van het toetsenbord tweemaal aan en uit. Op het scherm verschijnt een bericht over het herstel van het ROM met behulp van het opstartblok (dit geldt alleen voor bepaalde modellen).

In de herstelstand kunt u het systeem als volgt herstellen:

1. Verwijder eventuele diskettes uit de diskettedrive en schakel de stroom uit.
2. Plaats een ROMPaq diskette in de diskettedrive.
3. Schakel de stroom voor het systeem weer in.
4. Als geen ROMPaq diskette wordt aangetroffen, wordt u gevraagd deze in de diskettedrive te plaatsen en de computer opnieuw op te starten.
5. Als een instelwachtwoord is gedefinieerd, gaat het Caps Lock-lampje branden en wordt u gevraagd het wachtwoord in te voeren.
6. Voer het instelwachtwoord in.
7. Als het systeem goed vanaf diskette opstart en het systeem-ROM met succes herprogrammeert, gaan de drie lampjes van het toetsenbord branden. Een succesvolle bewerking wordt ook aangegeven door een serie geluidssignalen met stijgende toonhoogte.

Om te controleren of de ROM-flash geslaagd is, voert u de onderstaande stappen uit:

1. Plaats een geldige ROMPaq diskette in de diskettedrive.
2. Schakel de stroom voor het systeem uit.
3. Schakel de stroom voor het systeem in om de ROM-flash uit te voeren.
4. Als de ROM-flash met succes is uitgevoerd, gaan alle drie de toetsenbordlampjes branden en hoort u een reeks geluidssignalen die steeds hoger worden.
5. Verwijder de diskette, schakel de computer uit en start de computer opnieuw op.

In de volgende tabel vindt u een overzicht van de verschillende combinaties van toetsenbordlampjes die door het Boot Block ROM worden gebruikt, met hun betekenis en de maatregelen die erbij horen.

Combinaties van toetsenbordlampjes, gebruikt door het Boot Block ROM

FailSafe Boot Block-stand	Kleur toetsen-bordlampje	Toetsenbord Activiteit	Status/bericht
NumLock	Groen	Aan	ROMPaq diskette is niet aanwezig of is niet goed, of diskettedrive is niet gereed.*
Caps Lock	Groen	Aan	Voer een wachtwoord in.*
Num, Caps, Scroll Lock	Groen	Gaan 2 maal aan en uit (en er klinken 1 lang geluidssignaal en 3 korte geluidssignalen)	ROM-flash mislukt.*
Num, Caps, Scroll Lock	Groen	Aan	Boot Block ROM-flash met succes uitgevoerd. Zet het systeem uit en start opnieuw op.

✎ Diagnostische lampjes knipperen niet op USB-toetsenborden.

Computerinstellingen kopiëren

Deze procedure biedt een beheerder de mogelijkheid om op eenvoudige wijze een computerconfiguratie te kopiëren naar andere computers van hetzelfde type. Hierdoor kunnen meerdere computers sneller en consistenter worden geconfigureerd. U kopieert de computerinstellingen als volgt:

1. Ga met F10 naar het hulpprogramma Computer Setup (Computerinstellingen).
2. Klik op **File (Bestand) > Save to Diskette (Opslaan op diskette).** Volg de instructies op het scherm op.

Hiervoor heeft u een interne diskettedrive of een draagbare externe diskettedrive nodig.

3. Klik op **File (Bestand) > Restore from Diskette (Terugzetten vanaf diskette)** om de configuratie te kopiëren en volg de instructies op het scherm.

Altiris eXpress, System Software Manager en PC Transplant maken het eenvoudig om de configuratie en de aangepaste instellingen van de ene computer te kopiëren naar een of meer andere computers. Raadpleeg voor meer informatie de website http://www.compaq.com/easydeploy.

Aan/uit-knop met twee standen

Als Advanced Configuration and Power Interface (ACPI) is ingeschakeld voor Windows 98, Windows 2000, Windows ME en Windows XP, kan de aan/uit-knop functioneren als een aan/uit-schakelaar of als een standbyknop. In de standbystand wordt de voeding niet helemaal afgesloten maar verbruikt de computer minder energie. Hierdoor kunt u snel het stroomverbruik beperken zonder dat u applicaties hoeft te sluiten en kan de computer snel naar de oorspronkelijke stand terugkeren zonder dat u gegevens verliest.

U wijzigt de configuratie van de aan/uit-knop als volgt:

1. In Windows 2000 klikt u op **Start** en vervolgens selecteert u **Instellingen > Configuratiescherm > Energiebeheer.**

   In Windows XP klikt u op **Start** en vervolgens selecteert u **Configuratiescherm > Prestaties en onderhoud > Energiebeheer.**

2. Selecteer het tabblad **Geavanceerd** in het venster **Eigenschappen voor Energiebeheer.**

3. Selecteer de gewenste optie voor het energiebeheer.

Als u de aan/uit-knop eenmaal heeft geconfigureerd als standby-knop, kunt u met deze knop overschakelen op een stand met een bijzonder laag energieverbruik. Druk nogmaals op deze knop om weer terug te gaan naar de maximale stroomvoorziening. Als u de stroomvoorziening helemaal wilt uitschakelen, houdt u de aan/uit-knop vier seconden ingedrukt.

Energiebeheer

Met de voorziening Energiebeheer kunt u zonder de computer helemaal uit te zetten energie besparen door bepaalde onderdelen van de computer uit te schakelen als deze niet worden gebruikt.

Als ACPI (Advanced Configuration and Power Interface) in Windows 98, Windows 2000, Windows ME of Windows XP is ingeschakeld, kunt u via het besturingssysteem time-outperioden (een periode van inactiviteit die verstrijkt alvorens de onderdelen worden uitgeschakeld) inschakelen, aanpassen of uitschakelen.

1. In Windows 2000 klikt u op **Start** en vervolgens selecteert u **Instellingen > Configuratiescherm > Energiebeheer.**

   In Windows XP klikt u op **Start** en vervolgens selecteert u **Configuratiescherm > Prestaties en onderhoud > Energiebeheer.**

2. Selecteer het tabblad **Energiebeheerschema's** in het venster **Eigenschappen voor Energiebeheer.**

3. Selecteer de gewenste instellingen voor het energiebeheerschema.

Gebruik Eigenschappen voor Beeldscherm om de instellingen voor Energiebeheer van de monitor te definiëren, te wijzigen of uit te schakelen. U gaat naar Eigenschappen voor Beeldscherm door met de rechtermuisknop te klikken op het bureaublad van Windows en vervolgens **Eigenschappen** te selecteren.

Website

HP zorgt voor uitgebreide tests en debugprocedures van software die door HP of andere leveranciers is ontwikkeld. Bovendien ontwikkelt HP ondersteunende software specifiek voor elk besturingssysteem zodat HP computers optimaal presteren op het gebied van snelheid, compatibiliteit en betrouwbaarheid.

Wanneer u overschakelt naar een ander besturingssysteem of naar een nieuwere versie van het besturingssysteem, is het belangrijk om de ondersteunende software te implementeren die is ontwikkeld voor het betreffende besturingssysteem of de betreffende versie. Als u een andere versie van Microsoft Windows wilt gebruiken dan de versie die bij de computer is geleverd, is het noodzakelijk dat u de overeenkomstige stuurprogramma's en hulpprogramma's installeert zodat alle voorzieningen worden ondersteund en naar behoren functioneren.

Het is heel gemakkelijk om de meest recente versies van de HP ondersteunende software te vinden, te verkrijgen, uit te proberen en te installeren. U kunt de software downloaden vanaf http://www.compaq.com.

De websites bevatten de meest recente versie van stuurprogramma's, hulpprogramma's en flash-ROM-images die nodig zijn om het meest recente Microsoft Windows-besturingssysteem op uw HP computer te gebruiken.

Bouwstenen en partners

HP oplossingen voor beheer zijn gebaseerd op industriestandaarden, zoals DMI 2.0, Web-Based Enterprise Management, Intel's Wired for Management (WfM), SNMP en PXE (preboot execution environment). Microsoft, Intel, Altiris en andere marktleiders werken nauw samen met HP om hun beheeroplossingen te integreren met HP producten, waardoor de klanten van HP kunnen profiteren van geavanceerde Intelligent Manageability-oplossingen voor personal computers. Voor meer informatie bezoekt u http://www.compaq.com/easydeploy.

Desktop Management Interface (DMI)

De Desktop Management Task Force (DMTF) is een organisatie die is opgericht in 1992 met als doel de standaardisatie van systeembeheer. DMTF heeft het DMI-kader (Desktop Management Interface) gedefinieerd om de toegang tot de configuratiegegevens van computers te standaardiseren. HP is lid van de stuurgroep en de technische commissie van de DMTF en levert hardware en software die de DMI-standaard ondersteunen.

Raadpleeg het Help-bestand *Intelligent Manageability (Client Management)* voor meer informatie over het configureren van DMI-software.

Wired for Management

Wired for Management van Intel is gericht op beperking van de kosten voor ondersteuning en beheer van systemen met een Intel-architectuur, zonder dat dit afbreuk doet aan de flexibiliteit en de prestaties. De richtlijnen van Wired for Management bieden een basisset bouwstenen die door HP worden gebruikt in Intelligent Manageability (Client Management) voor gestandaardiseerd beheer van desktopcomputers, systeemconfiguratie op afstand, onderhoud op tijdstippen dat systemen niet in gebruik zijn en innovatief energiebeheer. Maar HP biedt meer dan alleen deze basisset. Intelligent Manageability is uitgerust met extra voorzieningen. Zo beschikt u over een uitgebreide oplossing voor het beheren van netwerkomgevingen.

De technologieën van Wired for Management zijn:

- Desktop Management Interface (DMI) 2.0
- Remote System Installation (Systeeminstallatie op afstand)
- Remote Wakeup and Remote Shutdown (Activeren en Afsluiten op afstand)
- ACPI-hardware
- SMBIOS
- PXE-ondersteuning (Pre-boot Execution)

Inventarisbeheer en beveiliging

Met de AssetControl voorzieningen van de computer beschikt u over essentiële inventarisatiegegevens die u kunt beheren met producten van HP Insight Manager en van Management Solutions Partners. Door de naadloze, automatische integratie van de voorzieningen van AssetControl in deze producten kunt u een hulpprogramma voor computerbeheer kiezen dat het beste aansluit op uw omgeving zodat uw investering in bestaande hulpprogramma's behouden blijft.

HP computers bevatten de hardware en firmware die is vereist voor volledige ondersteuning van de DMI 2.0-standaard.

HP biedt ook mogelijkheden om de toegang tot waardevolle onderdelen en informatie te beveiligen. Met behulp van beveiligingsvoorzieningen als Smart Cover Sensor en Smart Cover Lock, die op bepaalde modellen beschikbaar zijn, kunt u ongeoorloofde toegang tot de interne onderdelen van de computer voorkomen. Door parallelle poorten, seriële poorten of USB-poorten uit te schakelen of door het onmogelijk te maken om de computer op te starten vanaf een verwisselbare schijfeenheid, kunt u waardevolle gegevens beschermen. Waarschuwingen bij geheugenwijzigingen en waarschuwingen van de Smart Cover Sensor kunnen automatisch worden doorgestuurd naar HP Insight Manager producten, zodat geknoei met de interne onderdelen van een computer vroegtijdig wordt gemeld.

Op bepaalde systemen zijn Smart Cover Sensor en Smart Cover Lock als optie leverbaar.

Er zijn verschillende manieren waarop beveiligingsinstellingen op HP computers kunnen worden beheerd:

- Lokaal, met het hulpprogramma Computer Setup (Computerinstellingen). Zie de *Handleiding Computerinstellingen* voor aanvullende informatie en instructies voor het gebruik van dit hulpprogramma.
- Op afstand, met SSM (System Software Manager). SSM biedt veilige, consistente implementatie en besturing van beveiligingsinstellingen met behulp van een eenvoudig hulpprogramma.

In de volgende tabel en gedeelten vindt u informatie over het lokale beheer van beveiligingsvoorzieningen op de computer, via het hulpprogramma Computer Setup (Computerinstellingen).

Overzicht van beveiligingsvoorzieningen

Voorziening	Functie	In te stellen via
Opstartbeveiliging verwisselbare schijfeenheden	Voorkomt opstarten vanaf de verwisselbare schijfeenheden.	Vanuit Computer Setup (Computerinstellingen).
Beveiliging parallelle, seriële, USB- en infraroodpoorten	Voorkomt gegevensoverdracht via de geïntegreerde seriële en parallelle poort en de USB-(Universal Serial Bus) en infraroodpoort.	Vanuit Computer Setup (Computerinstellingen).
Power-On Password (Opstartwachtwoord)	Voorkomt dat de computer kan worden gebruikt als het wachtwoord niet is ingevoerd. Dit kan zowel van toepassing zijn bij het eerste opstarten van het systeem als bij het opnieuw starten.	Vanuit Computer Setup (Computerinstellingen).
Setup Password (Instelwachtwoord)	Voorkomt dat de configuratie wordt gewijzigd (via Computerinstellingen), tenzij het wachtwoord wordt ingevoerd.	Vanuit Computer Setup (Computerinstellingen).

Overzicht van beveiligingsvoorzieningen *(vervolg)*

Voorziening	Functie	In te stellen via
Netwerkserverstand	Biedt unieke beveiligingsfuncties voor computers die als server worden gebruikt.	Vanuit Computer Setup (Computerinstellingen).
DriveLock	Beschermt gegevens op specifieke vaste schijven tegen onbevoegd gebruik. Deze functie is niet op alle modellen beschikbaar.	Vanuit Computer Setup (Computerinstellingen).
Smart Cover Sensor	Geeft een waarschuwing als de kap of het zijpaneel van de computer verwijderd is geweest. U kunt deze optie zo instellen dat de gebruiker het instelwachtwoord moet invoeren om de computer opnieuw te kunnen opstarten nadat de kap of het zijpaneel is verwijderd. Raadpleeg de *Handleiding voor de hardware* op de cd *Documentation Library* voor meer informatie.	Vanuit Computer Setup (Computerinstellingen).
Master Boot Record Security (MBR-beveiliging)	Kan onbedoelde of opzettelijke wijzigingen in de hoofdopstartrecord (Master Boot Record, MBR) van de huidige opstartschijf voorkomen en maakt herstel van de vorige, ongewijzigde MBR mogelijk.	Vanuit Computer Setup (Computerinstellingen).

Overzicht van beveiligingsvoorzieningen *(vervolg)*

Voorziening	Functie	In te stellen via
Waarschuwingen bij geheugenwijziging	Controleert of geheugenmodules zijn toegevoegd, verplaatst of verwijderd en stelt in die gevallen zowel de eindgebruiker als de systeembeheerder op de hoogte.	Raadpleeg de online handleiding *Intelligent Manageability* voor informatie over het inschakelen van waarschuwingen bij geheugenwijzigingen.
Eigendomslabel	Toont de door de systeembeheerder vastgelegde eigendomsinformatie tijdens het opstarten van de computer (beschermd met het instelwachtwoord).	Vanuit Computer Setup (Computerinstellingen).
Bevestigingspunt voor kabelslot	Door een kabelslot aan te brengen, voorkomt u dat onbevoegden toegang hebben tot de binnenkant van de computer en zo de configuratie kunnen wijzigen of onderdelen kunnen verwijderen. U kunt een kabelslot ook gebruiken om de computer vast te leggen aan een moeilijk verplaatsbaar object, ter voorkoming van diefstal.	Bevestig de computer met een kabelslot aan een moeilijk verplaatsbaar object.

Overzicht van beveiligingsvoorzieningen *(vervolg)*

Voorziening	Functie	In te stellen via
Bevestigingspunt voor hangslot	Door een hangslot aan te brengen, voorkomt u dat onbevoegden toegang hebben tot de binnenkant van de computer en zo de configuratie kunnen wijzigen of onderdelen kunnen verwijderen.	Installeer een hangslot om ongewenste configuratiewijzigingen of verwijdering van componenten te voorkomen.

✎ Raadpleeg de *Handleiding Computerinstellingen* voor meer informatie over Computer Setup (Computerinstellingen).

Welke beveiligingsopties precies worden ondersteund, is afhankelijk van de computerconfiguratie.

Wachtwoordbeveiliging

Het opstartwachtwoord voorkomt dat onbevoegden de computer kunnen gebruiken. Telkens wanneer een gebruiker de computer inschakelt of opnieuw opstart, moet de gebruiker een wachtwoord invoeren om toegang te krijgen tot applicaties of gegevens. Het instelwachtwoord voorkomt specifiek onbevoegde toegang tot het hulpprogramma Computer Setup (Computerinstellingen) en kan ook worden gebruikt om het opstartwachtwoord te negeren. Dit betekent dat als u het instelwachtwoord invoert wanneer om het opstartwachtwoord wordt gevraagd, u toch toegang krijgt tot de computer.

Er kan een voor het hele netwerk geldig instelwachtwoord worden ingesteld om de systeembeheerder in staat te stellen zich aan te melden op alle netwerksystemen om onderhoud uit te voeren, zonder het opstartwachtwoord te hoeven kennen, ook al is er een ingesteld.

Instelwachtwoord definiëren met Computer Setup (Computerinstellingen)

U kunt een instelwachtwoord definiëren met behulp van Computer Setup (Computerinstellingen). Zo voorkomt u dat de configuratie (via Computerinstellingen) wordt gewijzigd zonder dat het wachtwoord wordt ingevoerd.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Setup Password (Instelwachtwoord)** en volg de instructies op het scherm.
4. Klik op **File** (Bestand) > **Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Opstartwachtwoord definiëren met Computer Setup (Computerinstellingen)

Het opstartwachtwoord is een beveiligingsvoorziening waarmee de computer alleen kan worden gebruikt als eerst een wachtwoord wordt ingevoerd. Als u een opstartwachtwoord heeft ingesteld, verschijnt de opdracht Password Options (Wachtwoordopties) in het menu Security (Beveiliging). Met deze opdracht kunt u de opties Network Server Mode (Netwerkserverstand) en Password Prompt on Warm Boot (Wachtwoordprompt bij warme start) selecteren.

Als de netwerkserverstand is uitgeschakeld, moet u telkens wanneer u de computer aan zet, het wachtwoord invoeren wanneer het sleutelpictogram op het scherm verschijnt. Als Password Prompt on Warm Boot is ingeschakeld, moet u het wachtwoord ook invoeren telkens wanneer u de computer opnieuw opstart. Als de netwerkserverstand is ingeschakeld, wordt u niet om het wachtwoord gevraagd tijdens POST, maar blijft een eventueel aangesloten PS/2-toetsenbord vergrendeld tot u het opstartwachtwoord heeft ingevoerd.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Power-On Password (Opstartwachtwoord)** en volg de instructies op het scherm.
4. Klik op **File (Bestand)** > **Save Changes** and **Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Opstartwachtwoord invoeren

U voert als volgt een opstartwachtwoord in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het huidige wachtwoord en drukt u op **Enter**.

Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Instelwachtwoord invoeren

Als er een instelwachtwoord op de computer is gedefinieerd, wordt u gevraagd dit in te voeren wanneer u Computer Setup (Computerinstellingen) wilt uitvoeren.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Wanneer de melding F10 = Setup in de rechterbenedenhoek van het scherm wordt weergegeven, drukt u op **F10**.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het instelwachtwoord en drukt u op **Enter**.

Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Opstart- of instelwachtwoord wijzigen

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**. Start Computer Setup (Computerinstellingen) om het instelwachtwoord te wijzigen.
2. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander begrenzingsteken, het nieuwe wachtwoord, nog een schuine streep (/) of een ander begrenzingsteken en tot slot nogmaals het nieuwe wachtwoord, zoals hieronder wordt weergegeven: **huidig wachtwoord/ nieuw wachtwoord/nieuw wachtwoord**

Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

3. Druk op **Enter**.

Het nieuwe wachtwoord wordt van kracht als u de computer opnieuw aan zet.

Zie het gedeelte “Scheidingstekens voor landspecifieke toetsenborden” in dit hoofdstuk voor informatie over alternatieve scheidingstekens. U kunt het opstartwachtwoord en het instelwachtwoord ook wijzigen met behulp van de beveiligingsopties in Computer Setup (Computerinstellingen).

Opstart- of instelwachtwoord verwijderen

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**. Start Computer Setup (Computerinstellingen) om het instelwachtwoord te verwijderen.
2. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander scheidingsteken, zoals hieronder wordt weergegeven: **huidig wachtwoord/**
3. Druk op **Enter**.

Zie het gedeelte "Scheidingstekens voor landspecifieke toetsenborden" voor informatie over alternatieve scheidingstekens. U kunt het opstartwachtwoord en het instelwachtwoord ook wijzigen met behulp van de beveiligingsopties in Computer Setup (Computerinstellingen).

Scheidingstekens en landspecifieke toetsenborden

Elk toetsenbord is ontworpen om tegemoet te komen aan landspecifieke vereisten. De syntaxis en de toetsen die u gebruikt om een wachtwoord te wijzigen of te verwijderen zijn afhankelijk van het toetsenbord dat bij de computer is geleverd. In Nederland wordt meestal gebruik gemaakt van het toetsenbord VS/Internationaal.

Scheidingstekens en landspecifieke toetsenborden

Arabisch	/	Grieks	–	Russisch	/
Belgisch	=	Hebreeuws	.	Slowaaks	–
BHKSJ*	–	Hongaars	–	Spaans	–
Braziliaans	/	Italiaans	–	Zweeds/Fins	/
Chinees	/	Japans	/	Zwitsers	–
Tsjechisch	–	Koreaans	/	Taiwanees	/
Deens	–	Latijns-Amerikaans	–	Thais	/
Frans	!	Noors	–	Turks	.
Canadees (Frans)	é	Pools	–	Engels (GB)	/
Duits	–	Portugees	–	VS/Internationaal	/

*Voor Bosnië-Herzegovina, Kroatië, Slovenië en Joegoslavië

Wachtwoorden wissen

Als u het wachtwoord bent vergeten, heeft u geen toegang tot de computer. Raadpleeg de handleiding *Problemen oplossen* voor informatie over het wissen van wachtwoorden.

Netwerkserverstand

De netwerkserverstand biedt unieke beveiligingsfuncties voor computers die als server worden gebruikt. Deze stand is alleen beschikbaar als een opstartwachtwoord is ingesteld via Computer Setup (Computer-instellingen). Als de netwerkserverstand is ingeschakeld, hoeft u het opstartwachtwoord niet in te voeren om vanaf de vaste schijf op te starten en hoeft er geen toetsenbord op het systeem te zijn aangesloten. Als er een PS/2-toetsenbord is aangesloten, blijft dit vergrendeld tot u het opstartwachtwoord heeft ingevoerd. Als een USB-toetsenbord is aangesloten, kunt u dit gewoon gebruiken. Als u wilt voorkomen dat het USB-toetsenbord wordt gebruikt nadat het besturingssysteem is geladen, verbergt u de USB-poort met behulp van de optie Device Security (Apparaatbeveiliging) in het menu Security (Beveiliging) van Computer Setup (Computerinstellingen). Als u de netwerkserverstand in combinatie met de opstartoptie After Power Loss (Na stroomonderbreking) van Computer Setup (Computerinstellingen) gebruikt, kan de “server” na een stroomonderbreking automatisch opnieuw opstarten zonder interactie van de gebruiker. Als de netwerkserverstand is ingeschakeld, is het noodzakelijk om het opstartwachtwoord in te voeren om op te starten vanaf verwisselbare media (bijvoorbeeld diskettes) of verwisselbare apparaten (bijvoorbeeld USB-flash-apparaten).

DriveLock

DriveLock is een beveiligingsvoorziening die ongeoorloofde toegang tot gegevens op specifieke vaste schijven voorkomt. DriveLock is geprogrammeerd als een uitbreiding van Computer Setup (Computer-instellingen). Deze functie is niet op alle systemen beschikbaar en kan alleen worden gebruikt wanneer vaste schijven worden gedetecteerd die compatibel zijn met DriveLock.

DriveLock is bedoeld voor gebruikers van HP systemen voor wie gegevensbeveiliging van het allergrootste belang is. Voor deze gebruikers zijn de kosten van de vaste schijf en het verlies van de gegevens op de schijf irrelevant vergeleken bij de schade die zou kunnen ontstaan bij ongeoorloofde toegang tot de inhoud van de schijf. DriveLock maakt gebruik van een beveiligingsschema met twee wachtwoorden om dit beveiligingsniveau toe te passen en tegelijkertijd rekening te houden met de mogelijkheid dat een wachtwoord wordt vergeten. Het ene wachtwoord wordt ingesteld en gebruikt door de systeembeheerder, het andere wordt doorgaans ingesteld en gebruikt door de eindgebruiker. Er is geen noodoplossing beschikbaar: als u beide wachtwoorden vergeet, kan de schijfeenheid niet meer worden ontgrendeld. Daarom wordt u aangeraden de gegevens op de vaste schijf te kopiëren naar een bedrijfsinformatiesysteem of er regelmatig een backup van te maken.

Als u beide DriveLock wachtwoorden vergeet, kan de vaste schijf niet meer worden gebruikt. Voor gebruikers die niet beantwoorden aan het hierboven gedefinieerde profiel, is dit risico mogelijk niet acceptabel. Voor gebruikers die wel beantwoorden aan dit profiel, is dit risico mogelijk acceptabel vanwege het type gegevens op de vaste schijf.

DriveLock gebruiken

De optie DriveLock staat in het menu Security (Beveiliging) van Computer Setup (Computerinstellingen). U kunt kiezen uit opties om het hoofdwachtwoord in te stellen of DriveLock in te schakelen. Om DriveLock te kunnen inschakelen, moet een gebruikerswachtwoord worden opgeven. Aangezien de initiële configuratie van DriveLock doorgaans wordt uitgevoerd door de systeembeheerder, stelt u wellicht eerst een hoofdwachtwoord in. De systeembeheerder wordt aangeraden altijd een hoofdwachtwoord in te stellen, ongeacht of DriveLock wordt ingeschakeld. Hierdoor kan de systeembeheerder de instellingen van DriveLock wijzigen als de schijfeenheid in de toekomst wordt vergrendeld. Nadat het hoofdwachtwoord is ingesteld, kan de systeembeheerder desgewenst DriveLock inschakelen.

Als het systeem een vergrendelde vaste schijf bevat, wordt u tijdens POST gevraagd een wachtwoord in te voeren om de schijf te ontgrendelen. Als een opstartwachtwoord is ingesteld en dit overeenkomt met het gebruikerswachtwoord voor de schijf, wordt u niet gevraagd het wachtwoord nogmaals in te voeren. Als twee verschillende wachtwoorden worden gebruikt, wordt u wel gevraagd een DriveLock wachtwoord in te voeren. Gebruik hiervoor het hoofdwachtwoord of het gebruikerswachtwoord. U mag één keer een verkeerd wachtwoord invoeren. Als u twee keer een verkeerd wachtwoord invoert, wordt POST verder uitgevoerd maar heeft u geen toegang tot de gegevens op de schijf.

Toepassingen van DriveLock

Het meest voorkomende gebruik van de beveiligingsvoorziening DriveLock is in een bedrijfsomgeving waarbij een systeembeheerder MultiBay-vaste schijven gebruikt in bepaalde computers. De systeembeheerder is doorgaans verantwoordelijk voor het configureren van de MultiBay vaste schijven, zoals het instellen van het DriveLock hoofdwachtwoord. Als een gebruiker het gebruikerswachtwoord vergeet of de apparatuur door een andere werknemer wordt gebruikt, kan het hoofdwachtwoord worden gebruikt om het gebruikerswachtwoord opnieuw in te stellen zodat de gegevens op de vaste schijf opnieuw toegankelijk worden.

Systeembeheerders van bedrijven die DriveLock willen gebruiken, wordt aangeraden ook een bedrijfsbeleid toe te passen voor het instellen en bijhouden van hoofdwachtwoorden, om te voorkomen dat een werknemer met opzet of per ongeluk beide DriveLock wachtwoorden instelt voordat hij of zij het bedrijf verlaat. In dat geval zou de vaste schijf onbruikbaar zijn en moeten worden vervangen. Als de systeembeheerder geen hoofdwachtwoord instelt, is het ook mogelijk dat de beheerder geen toegang meer heeft tot een vaste schijf en geen routinecontroles kan uitvoeren op ongeoorloofde software, andere functies voor inventarisbeheer en ondersteuning.

Als u minder strikte beveiligingsvereisten heeft, wordt u afgeraden DriveLock in te schakelen. Dit geldt voor privé-gebruikers of gebruikers die doorgaans geen vertrouwelijke gegevens op hun vaste schijf hebben. Voor deze gebruikers is het mogelijke verlies van een vaste schijf wanneer beide wachtwoorden zijn vergeten, van veel groter belang dan de waarde van de gegevens die door DriveLock worden beveiligd. Gebruik het instelwachtwoord om de toegang tot Computer Setup (Computerinstellingen) en DriveLock te beperken. Door een instelwachtwoord op te geven maar dit niet aan de eindgebruiker mee te delen, kan de systeembeheerder voorkomen dat andere gebruikers DriveLock inschakelen.

Smart Cover Sensor

De Smart Cover Sensor die op bepaalde modellen beschikbaar is, is een combinatie van hardware- en softwaretechnologie die u waarschuwt als de kap of het zijpaneel van de computer is verwijderd. Er zijn drie beveiligingsniveaus, zoals beschreven in onderstaande tabel:

Beveiligingsniveaus van Smart Cover Sensor

Niveau	Instelling	Beschrijving
Niveau 0	Disabled(Uitgeschakeld)	De Smart Cover Sensor is uitgeschakeld (standaardinstelling).
Niveau 1	Notify User (Gebruiker waarschuwen)	Bij het opnieuw starten van de computer verschijnt het bericht dat de kap of het zijpaneel van de computer verwijderd is geweest.
Niveau 2	Setup Password (Instelwachtwoord)	Bij het opnieuw starten van de computer verschijnt het bericht dat de kap of het zijpaneel van de computer verwijderd is geweest. Om door te kunnen gaan, moet het instelwachtwoord worden ingevoerd.

✎ Deze instellingen kunnen worden gewijzigd met behulp van Computer Setup (Computerinstellingen). Raadpleeg de *Handleiding Computerinstellingen* voor meer informatie over dit hulpprogramma.

Beveiligingsniveau van Smart Cover Sensor instellen

U stelt als volgt het beveiligingsniveau van de Smart Cover Sensor in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Smart Cover** en volg de instructies op het scherm.
4. Klik op **File (Bestand) > Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Smart Cover Lock

Het Smart Cover Lock is een softwarematige kapbeveiliging waarmee sommige HP computers zijn uitgerust. Met dit slot wordt voorkomen dat onbevoegden toegang krijgen tot de interne onderdelen. Bij levering van de computer is het Smart Cover Lock niet vergrendeld.

VOORZICHTIG: U wordt aangeraden een instelwachtwoord te definiëren voor maximale beveiliging. Het instelwachtwoord voorkomt dat onbevoegden de computerconfiguratie kunnen wijzigen via Computer Setup (Computerinstellingen).

Het Smart Cover Lock is op bepaalde modellen als optie leverbaar.

Smart Cover Lock vergrendelen

U kunt als volgt het Smart Cover Lock activeren en vergrendelen:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer achtereenvolgens **Security (Beveiliging), Smart Cover** en de optie **Locked (Vergrendelen).**
4. Klik op **File (Bestand) > Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Smart Cover Lock ontgrendelen

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer **Security (Beveiliging) > Smart Cover > Unlocked (Ontgrendelen).**
4. Klik op **File (Bestand) > Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Smart Cover FailSafe-sleutel

Als u het Smart Cover Lock heeft ingeschakeld, maar het wachtwoord niet kunt invoeren om de beveiliging uit te schakelen, heeft u een Smart Cover FailSafe-sleutel nodig om de kap van de computer te openen. U gebruikt de sleutel in één van de volgende situaties:

- Stroomstoring
- Opstartstoring
- Bij een storing in een onderdeel van de computer (zoals de processor of voedingseenheid)
- U bent het wachtwoord vergeten

VOORZICHTIG: De Smart Cover FailSafe-sleutel is bij HP verkrijgbaar. Bestel deze sleutel uit voorzorg, vóórdat u deze daadwerkelijk nodig heeft. De sleutel is verkrijgbaar bij HP Business of Service Partners onder bestelnummer PN 166527-001 voor het moersleuteltype of PN 166527-002 voor het schroevendraaiertype.

U kunt de FailSafe-sleutel als volgt aanschaffen:

- Neem contact op met een geautoriseerde HP Business of Service Partner.
- Bezoek http://www.compaq.com voor bestelinformatie.
- Bel het telefoonnummer dat bij het garantiebewijs wordt genoemd.

Raadpleeg de *Handleiding voor de hardware* voor meer informatie over de Smart Cover FailSafe-sleutel.

Master Boot Record Security

De Master Boot Record (MBR, hoofdopstartrecord) bevat informatie die nodig is om vanaf een schijf te kunnen opstarten en toegang te krijgen tot de gegevens op die schijf. Via Master Boot Record Security (MBR-beveiliging) kunnen onbedoelde of opzettelijke wijzigingen in de MBR worden voorkomen, zoals wijzigingen die worden veroorzaakt door bepaalde computervirussen of door onjuist gebruik van bepaalde schijfhulpprogramma's. Ook kunt u hiermee de vorige, ongewijzigde MBR herstellen, indien er wijzigingen in de MBR worden gedetecteerd wanneer het systeem opnieuw wordt opgestart.

U schakelt MBR-beveiliging als volgt in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer **Security (Beveiliging) > Master Boot Record Security (MBR-beveiliging) > Enabled (Inschakelen).**
4. Selecteer **Security (Beveiliging) > Save Master Boot Record (MBR opslaan).**
5. Klik op **File (Bestand) > Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Wanneer de MBR-beveiliging is ingeschakeld, wordt via het BIOS voorkomen dat in de MS-DOS-stand of de Veilige modus van Windows wijzigingen worden aangebracht in de MBR van de huidige opstartschijf.

De meeste besturingssystemen regelen de toegang tot de MBR van de huidige opstartschijf. Het BIOS kan geen wijzigingen voorkomen die worden aangebracht terwijl het besturingssysteem actief is.

Wanneer de computer wordt ingeschakeld of opnieuw wordt opgestart, wordt de MBR van de huidige opstartschijf door het BIOS vergeleken met de laatst opgeslagen MBR. Als hierbij wijzigingen worden aangetroffen en de huidige opstartschijf dezelfde is als de schijf waarvan de MBR eerder is opgeslagen, wordt het volgende bericht weergegeven:

1999 – Master Boot Record has changed (MBR is gewijzigd).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- De MBR van de huidige opstartschijf opslaan.
- De eerder opgeslagen MBR herstellen.
- MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

Als wijzigingen worden aangetroffen terwijl de huidige opstartschijf **niet** de schijf is waarvan de MBR eerder is opgeslagen, wordt het volgende bericht weergegeven:

2000 – Master Boot Record Hard Drive has changed (Vaste schijf van MBR is gewijzigd).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- De MBR van de huidige opstartschijf opslaan.
- MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

Als de eerder opgeslagen MBR beschadigd is, wordt het volgende bericht weergegeven:

1998 – Master Boot Record has been lost (MBR is verloren gegaan).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- De MBR van de huidige opstartschijf opslaan.
- MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

Voordat u de huidige opstartschijf partitioneert of formatteert

Controleer of de MBR-beveiliging is uitgeschakeld voordat u de huidige opstartschijf opnieuw partitioneert of formatteert. Door sommige schijfhulpprogramma's, zoals FDISK en FORMAT, kan een update van de MBR worden uitgevoerd. Als u de schijf opnieuw partitioneert of formatteert terwijl de MBR-beveiliging is ingeschakeld, kan dit leiden tot foutberichten van het schijfhulpprogramma of tot een waarschuwing van MBR-beveiliging wanneer u de computer weer inschakelt of opnieuw opstart. U schakelt de MBR-beveiliging als volgt uit:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten.**
2. Druk op **F10** zodra het bericht F10 = Setup rechtsonder in het scherm verschijnt. Druk op **Enter** om een eventueel beginscherm over te slaan.

Als u niet op **F10** drukt voordat het bericht is verdwenen, start u de computer opnieuw op en probeert u opnieuw toegang te krijgen tot het hulpprogramma.

3. Selecteer **Security (Beveiliging) > Master Boot Record Security (MBR-beveiliging) > Disabled (Uitschakelen).**
4. Klik op **File (Bestand) > Save Changes** and **Exit (Wijzigingen opslaan** en **afsluiten)** voordat u het programma afsluit.

Kabelslot

De achterkant van de computer is voorzien van een bevestigingspunt voor een kabelslot, zodat de computer fysiek aan de werkplek kan worden bevestigd.

Raadpleeg de *Handleiding voor de hardware* op de cd *Documentation Library* voor geïllustreerde instructies.

Vingerafdruk-identificatietechnologie

Met de HP vingerafdruk-identificatietechnologie is het niet meer nodig dat de eindgebruiker wachtwoorden invoert en wordt de netwerkbeveiliging verbeterd. Bovendien wordt het aanmelden vereenvoudigd en nemen de beheerkosten van bedrijfsnetwerken af. Aangezien deze optie gunstig geprijsd is, is deze niet uitsluitend voorbehouden aan hightech-organisaties met behoefte aan strikte beveiliging.

Ondersteuning van de technologie voor vingerafdrukidentificatie is afhankelijk van het model.

Voor meer informatie bezoekt u http://www.compaq.com/products/quickspecs/10690_na/10690_na.html

Foutberichten en foutherstel

Deze computer is uitgerust met voorzieningen voor foutberichten en foutherstel waarbij innovatieve hardware- en softwaretechnologie voorkomt dat essentiële gegevens verloren gaan. Ook blijft ongeplande uitvaltijd van de apparatuur tot een minimum beperkt.

Wanneer zich een storing voordoet, verschijnt een lokale waarschuwing met een beschrijving van de fout en de aanbevolen acties. U kunt vervolgens de huidige systeemstatus bekijken met behulp van de HP Insight Management Agent. Als de computer is aangesloten op een netwerk dat wordt beheerd met een HP Insight Manager applicatie of andere applicaties voor netwerkbeheer van Management Solutions Partners, worden de foutberichten ook naar de desbetreffende applicatie gestuurd.

Schijfbeveiligingssysteem

Het schijfbeveiligingssysteem DPS is een diagnosehulpmiddel dat in de vaste schijf van bepaalde HP computers is ingebouwd. DPS is bedoeld om een diagnose te stellen van problemen met de vaste schijf, zodat de vaste schijf niet nodeloos wordt vervangen.

Tijdens de productie van HP bedrijfscomputers wordt elke geïnstalleerde vaste schijf met DPS getest en wordt de belangrijkste informatie permanent naar de schijf geschreven. Elke keer dat DPS wordt uitgevoerd, worden de testresultaten naar de vaste schijf geschreven. Geautoriseerde Compaq Business of Service Partners gebruiken deze informatie om de omstandigheden te achterhalen die het uitvoeren van DPS noodzakelijk maakten. Raadpleeg de handleiding *Problemen oplossen* voor informatie over het gebruik van DPS.

Ultra ATA Integrity Monitoring

Met Ultra ATA Integrity Monitoring wordt de integriteit van de gegevens gecontroleerd tijdens de overdracht van deze gegevens tussen een Ultra ATA-vaste schijf en het systeem. Als de computer een abnormale hoeveelheid verzendfouten detecteert, verschijnt een lokale waarschuwing met aanbevelingen om de fouten te voorkomen.

Netvoeding met spanningspiekbeveiliging

Een geïntegreerde voedingseenheid met beveiliging tegen spanningspieken biedt grotere betrouwbaarheid bij onverwachte spanningspieken. Hierdoor kan het systeem spanningspieken van maar liefst 2.000 V weerstaan zonder dat het systeem uitvalt of gegevens verloren gaan.

Temperatuursensor

De temperatuursensor is een hardware- en softwarematige voorziening die de interne temperatuur van de computer in de gaten houdt. Er verschijnt een waarschuwing wanneer het normale bereik wordt overschreden en u krijgt de gelegenheid om actie te ondernemen voordat interne onderdelen beschadigd raken of gegevens verloren gaan.

Index

T

U

V

W